ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ 2026

10 ПРАВИЛ ЦИФРОВОЇ БЕЗПЕКИ

Постав ✓ навпроти того, що вже зробив. Решту — зроби до кінця тижня!

1	**Менеджер паролів замість однакового пароля скрізь** Bitwarden (безкоштовно), 1Password або Keeper. Один майстер-пароль → унікальний пароль для кожного сайту.	☐
2	**Двофакторна аутентифікація (2FA) на пошті та соцмережах** Instagram, Gmail, TikTok, Steam → Налаштування → Безпека → Двоетапна перевірка. Authenticator App — надійніше за SMS.	☐
3	**Перевіряй URL перед введенням пароля або даних картки** Правильно: privatbank.ua. Фішинг: privat-ua.ru / privat24.tk. Один зайвий символ у домені = крадіжка даних.	☐
4	**Приватний профіль у соцмережах (або чистий публічний)** Instagram/TikTok → Налаштування → Приватний акаунт. Вимкни геолокацію, не публікуй розклад і місце навчання.	☐
5	**Не вводь дані картки на підозрілих сайтах** Перевір: є HTTPS (замок), знайомий домен, є контакти компанії. Для покупок — краще віртуальна картка або Apple/Google Pay.	☐
6	**VPN або мобільний інтернет у публічних місцях** Кафе, торговий центр, коледж — публічний Wi-Fi небезпечний. Безкоштовний VPN: ProtonVPN.	☐
7	**Перевір свій email на витік прямо зараз** Зайди на haveibeenpwned.com → введи email. Якщо знайшло витік — одразу зміни пароль і увімкни 2FA.	☐
8	**Домовся з сім'єю про «кодове слово» від deepfake** Придумайте секретне слово. Якщо «рідний» дзвонить і просить гроші — запитай кодове слово. ШІ не знатиме відповіді.	☐
9	**Регулярно оновлюй операційну систему і застосунки** Оновлення закривають вразливості, через які злочинці заходять у пристрій. Увімкни автооновлення.	☐
10	**Думай перш ніж публікувати — інтернет пам'ятає все** Правило 3 секунд: «Чи хочу я, щоб це побачили всі — через 10 років?» Видалення поста не видаляє скриншоти.	☐

ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ 2026

ПРАКТИЧНІ КЕЙСИ ДЛЯ ГРУПОВОГО ОБГОВОРЕННЯ

Робота в парах або мікрогрупах по 3–4 особи. Час на обговорення кожного кейсу — 5–7 хвилин.

КЕЙС №1 — Фішинг від «ПриватБанку»

Сценарій:

Аліна (16 років) отримала повідомлення в Instagram від акаунту @privat24.ukraine (3 підписники, аватар — логотип банку): «Вітаємо! Ваш рахунок обрано для отримання кешбеку ₴500 в рамках акції «Молодіжний бонус 2026». Для нарахування перейдіть за посиланням і підтвердіть картку: http://privat-bonus2026.ru/verify Увага! Акція діє лише 24 години.» Аліна хоче отримати гроші, але щось її зупиняє...

Питання для обговорення:

1. Які ознаки фішингу ви бачите? Знайдіть мінімум 4 «червоних прапорці».
2. Чому ₴500 — ефективна наживка? Як шахраї використовують психологію жертви?
3. Що Аліна має зробити прямо зараз? Сформулюйте покроковий алгоритм дій.
4. Якби Аліна клікнула — що сталося б далі з її картковими даними?

Відповіді для викладача:

Червоні прапорці: домен .ru (не .ua), акаунт з 3 підписниками, терміновість «24 години», Instagram — не офіційний канал банку, запит даних картки через посилання (банки так не роблять).

Психологія: несподівана вигода + терміновість = відключення критичного мислення. Жертва думає про гроші, а не про безпеку.

Що робити: 1) Не клікати. 2) Заблокувати і поскаржитись на акаунт. 3) Зателефонувати в банк за номером з картки. 4) Розказати рідним.

Якщо клікнула: потрапить на сайт-клон, де введе дані картки → рахунок спустошать за лічені хвилини. Деякі сайти також завантажують шкідливе ПЗ.

КЕЙС №2 — AI Deepfake: «Тато в небезпеці»

Сценарій:

Максиму (15 років) телефонує невідомий номер. Голос — точно татів, навіть характерна хрипотця є. «Тато» каже, що потрапив у ДТП, поліція вимагає ₴15 000 застави прямо зараз, інакше — арешт. Просить терміново переказати гроші «адвокату» Андрію. «Максиме, я не можу довго говорити — поруч слідчий. Зроби це ЗАРАЗ. Мамі не кажи.» Максим в паніці. Голос — справжній. Він точно знає, як тато говорить...

Питання для обговорення:

5. Як ШІ міг клонувати голос тата? Звідки шахраї взяли зразок голосу?
6. Чому не можна беззаперечно довіряти голосу у телефоні? Яка технологія за цим стоїть?
7. Знайдіть усі маніпулятивні елементи в сценарії.
8. Що Максим має зробити протягом 30 секунд? Покрокові дії під час дзвінка.

Відповіді для викладача:

Технологія: 10–30 секунд аудіо достатньо для клонування голосу (ElevenLabs, Resemble AI). Зразки беруть з TikTok, голосових у Telegram.

Маніпуляції: невідомий номер, терміновість, гроші через посередника, «не кажи мамі» (ізоляція жертви), «слідчий поруч» (тиск).

Дії: 1) Покласти слухавку. 2) Одразу зателефонувати татові на збережений номер. 3) Якщо не відповідає — зателефонувати іншим рідним. 4) Не переказувати гроші, поки не переконався.

Захист: домовтесь із сім'єю про «кодове слово» — питання/відповідь, яку знають тільки ви. ШІ не знатиме правильної відповіді.

КЕЙС №3 □ Витік акаунту Steam

Сценарій:

Олег (17 років) — заядлий геймер. Має Steam-акаунт з іграми на ₴12 000. В Discord приходить повідомлення від «друга» Юрка: «Олег, привіт! Тут є крутий сайт — роздають скіни CS2 безкоштовно. Я вже взяв два! Зайди: steam-skin-drop.net і залогінься через Steam.» Олег заходить. Сайт схожий на Steam — навіть логотип є. Вводить логін і пароль. Через 10 хвилин приходить сповіщення: «Вхід з нового пристрою, Мінськ». Олег намагається зайти — неправильний пароль...

Питання для обговорення:

9. Де Олег допустив помилку? Знайдіть усі точки, де він міг зупинитись.
10. Чому повідомлення прийшло саме від «Юрка»? Що сталося з акаунтом друга?
11. Що робити Олегу зараз — перші 5 хвилин? Сформулюйте термінові дії.
12. Які налаштування Steam захищають від повторення цієї ситуації?

Відповіді для викладача:

Помилки: перейшов за посиланням без перевірки; не перевірив URL (steam-skin-drop.net ≠ store.steampowered.com); не було 2FA; не уточнив у Юрка особисто.

Ланцюжок: зламали Юрка → отримали його контакти → розіслали від його імені → зібрали нові акаунти. Класичний «ланцюговий» фішинг.

Термінові дії: 1) Steam → «Забули пароль» → відновлення через email. 2) Змінити пароль email. 3) Steam → Налаштування → Активні сесії → завершити всі. 4) Звернутись у Steam Support. 5) Попередити друзів.

Захист: увімкнути Steam Guard (2FA через мобільний застосунок), ніколи не вводити дані на сторонніх сайтах, перевіряти URL перед входом.

КЕЙС №4 □ Публічні фото і доксинг

Сценарій:

Катя (16 років) веде публічний Instagram. Публікує фото у формі коледжу, stories «де я зараз», сімейні вечері з геолокацією «вдома». Одного дня незнайомець пише: «Привіт, Катю. Ти вчишся в [назва коледжу], живеш на [назва вулиці], щовівторка ходиш на фітнес

о 18:00, а твій тато працює в [назва компанії]. Це не складно дізнатись з твого Інстаграму. Ти не боїшся?» Катя в шоці — вся ця інформація справді є у неї у профілі...

Питання для обговорення:

13. Як незнайомець зібрав цю інформацію? Яке фото що розкриває?
14. Які ризики несе кожна «безневинна» публікація? Хто ще, крім шахраїв, може зловживати цим?
15. Що Катя може зробити прямо зараз? З чого почати аудит профілю?
16. Де межа між відкритістю і небезпекою? Чи можна вести публічний профіль і залишатись у безпеці?

Відповіді для викладача:

Збір даних: фото у формі → назва коледжу. Геолокація в stories → адреса. Теги → місця роботи батьків. Регулярні stories → розклад дня. EXIF-метадані фото → точні координати.

Ризики: сталкінг, пограбування (знають, коли нема вдома), шантаж, соціальна інженерія проти родини.

Дії: 1) Перейти на приватний акаунт. 2) Видалити геолокацію зі старих постів. 3) Вимкнути геодані в камері (Налаштування → Конфіденційність → Геолокація → Камера → Ніколи). 4) Не публікувати щоденний розклад.

Баланс: публічний профіль можна вести — але без геолокацій, розкладу та місця навчання у відкритому доступі. Публікуй де ТИ БУВ, а не де ТИ ЗАРАЗ.

Черкаський художньо-технічний фаховий коледж

ПЛАН-КОНСПЕКТ

проведення виховного заходу

Тема:	«День безпечного Інтернету 2026»
Форма проведення:	виховний захід (інтерактивне заняття)
Дата проведення:	25 лютого 2026 року
Тривалість:	45 хвилин
Місце проведення:	навчальна аудиторія 201
Учасники:	студенти 1 курсу
Відповідальний:	Сугак Володимир Олександрович

І. МЕТА ЗАХОДУ

Освітня мета: формування у студентів знань про актуальні кіберзагрози 2025–2026 років (фішинг, ШІ-шахрайство, витік персональних даних), способи їх розпізнавання та практичні алгоритми захисту.

Виховна мета: виховання відповідального ставлення до власної цифрової безпеки та безпеки оточуючих; усвідомлення особистої відповідальності за поведінку в інтернеті.

Розвивальна мета: розвиток критичного мислення при роботі з інформацією в мережі, вміння аналізувати підозрілий контент та приймати зважені рішення в ситуаціях кіберзагроз.

ІІ. ОБЛАДНАННЯ ТА МАТЕРІАЛИ

- мультимедійний проєктор та екран;
- презентація PowerPoint «День безпечного Інтернету 2026» (16 слайдів);
- роздатковий матеріал: чек-лист «10 правил цифрової безпеки» (по одному на кожного студента);
- роздруковані кейси для групового обговорення (4 сценарії);
- дошка або фліпчарт для фіксації відповідей.

ІІІ. ПЛАН ПРОВЕДЕННЯ

Загальна тривалість: 45 хвилин

Час	Етап	Зміст
0:00–0:05 (5 хв)	Організаційна частина	Привітання учасників. Анонімне опитування: «Хто стикався з підозрілими повідомленнями онлайн?» Встановлення зв'язку теми з особистим досвідом студентів.
0:05–0:12 (7 хв)	Актуалізація теми	Слайди 1–3. Статистика кіберзагроз в Україні за 2024–2025 роки (CERT-UA, Кіберполіція). Топ загроз 2025–2026. Запитання до аудиторії перед кожною цифрою: «Скільки, як думаєте?»

0:12–0:22 (10 хв)	Основний зміст: загрози та захист	Слайди 4–5. Розбір реального фішингового листа — студенти самостійно шукають «червоні прапорці». AI-deepfake дзвінки: технологія та метод захисту (кодове слово). Слайди 6–7. Інтерактив «Скільки часу злому пароля?». Двофакторна аутентифікація.
0:22–0:30 (8 хв)	Практична частина	Слайди 8–9. Цифрова тінь у соціальних мережах. Демонстрація сервісу haveibeenpwned.com. Кейси №1 і №2 — робота в парах, вибір правильного алгоритму дій.
0:30–0:38 (8 хв)	Поглиблення теми	Слайд 12. Небезпека публічного Wi-Fi: міф vs реальність. Кейси №3 і №4. Групова дискусія: що змінити у своїй цифровій поведінці прямо зараз?
0:38–0:43 (5 хв)	Закріплення знань	Слайд 13. Роздача чек-листу «10 правил». Кожен студент обирає 3 пункти, які виконає сьогодні. Слайд 14. Усний тест — 4 запитання.
0:43–0:45 (2 хв)	Підбиття підсумків	Слайди 15–16. Ресурси допомоги: Кіберполіція 0 800 505 170, cyberpolice.gov.ua. Фінальне повідомлення. Зворотній зв'язок від студентів.

IV. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

Заняття проводиться в неформальному, діалоговому форматі — без монологічних лекцій. Акцент робиться не на залякуванні загрозами, а на конкретних практичних діях: що зробити, щоб захиститись.

Під час розбору кейсів викладач надає слово різним студентам, заохочує висловлювати власну думку та аргументувати вибір. У разі неправильної відповіді — не критикує, а спрямовує до правильного висновку через додаткові запитання.

Якщо в аудиторії є доступ до інтернету — провести live-демонстрацію сервісу haveibeenpwned.com: запропонувати студентам добровільно перевірити власну електронну скриньку. Цей момент зазвичай справляє найбільше враження.

V. ОЧІКУВАНІ РЕЗУЛЬТАТИ

За підсумками заходу студенти мають:

- знати ознаки фішингових повідомлень і підроблених сайтів;
- розуміти, як працює AI-deepfake та чому не можна беззаперечно довіряти голосу у телефоні;
- вміти налаштувати двофакторну аутентифікацію в соціальних мережах;
- знати алгоритм дій при отриманні підозрілого дзвінка або повідомлення;
- знати, куди звертатися у разі кіберінциденту (0 800 505 170, cyberpolice.gov.ua).

VI. ВИКОРИСТАНІ ДЖЕРЕЛА ТА РЕСУРСИ

- CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події: cert.gov.ua;
- Департамент кіберполіції Національної поліції України: cyberpolice.gov.ua;
- Звіти Кіберполіції України про стан кіберзлочинності, 2024–2025 рр.;
- Сервіс перевірки витоків персональних даних: haveibeenpwned.com;
- Матеріали міжнародного Дня безпечного Інтернету 2026: saferinternetday.org.